LISTING OF CLAIMS

1. (Currently Amended) A system for duplicating documents of disparate types [to provide a] for facilitating searching [mechanism] of such documents, said system comprising:

storage means for storing at least one [an] original file, each containing no more than one original document, said original file being in a first format;

processing means [when] for determining that said original document is a component document of a compound document, [for] extracting said component document from said compound document and storing said component document in said original file; and

conversion means for converting said original file from said first format to a canonical format [to produce] thereby generating a duplicate file containing a duplicate document of said original document, whereby searching of such documents is facilitated.

2. (Currently Amended) A system for securely duplicating documents of disparate types [to provide a cyrptographically secure link between a duplicate document and an original document], said system comprising:

storage means for storing [an] at least one original file, each containing no more than one original document, said original file being in a first format;

conversion means for converting said original file from said first format to a canonical format [to produce] thereby generating a duplicate file containing a duplicate document of said original document;

embedding means for embedding notary data associated with said original file into [said canonical format of] said duplicate file, said notary data being capable of authenticating said original file; and

indexing means for inserting a unique sequence number including [part] at least a portion of said notary data into said duplicate file to provide a cryptographically secure link between said duplicate document and said original document.

3. (Original) The system of Claim 2, wherein said original document is a component document of a compound document, and further comprising:

processing means for extracting said component document from said compound document and storing said component document in said original file.

4. (Original) The system of Claim 3, wherein said storage means has a directory structure, said component document being stored in said storage means under a directory associated with said compound document.

5. (Original) The system of Claim 2, wherein said canonical format is the Portable Document Format (PDF).

6. (Original) The system of Claim 5, wherein said duplicate document has a Root Dictionary field therein, and further comprising:

creation means for creating a new Dictionary associated with said system; and

insertion means for storing said new Dictionary in said Root Dictionary field and inserting said notary data into said new Dictionary.

7. (Original) The system of Claim 2, wherein said notary data includes at least a digital fingerprint associated with said original file, a timestamp indicating the time said digital fingerprint was obtained and an identifier, said sequence number including said identifier.

8. (Original) The system of Claim 2, wherein said sequence number is inserted as a footer on the bottom of each page of said duplicate document.

9. (Original) The system of Claim 2, further comprising:

additional storage means for storing said duplicate file, said additional storage means having a directory format identical to the directory format of said storage means storing said original file.

10. (Original) The system of Claim 2, further comprising:

additional embedding means for embedding notary data associated with said duplicate file into said canonical format of said duplicate file, said notary data being capable of authenticating said duplicate file.

11. (Original) The system of Claim 2, further comprising:

a log file configured to map a sequenced filename associated with said duplicate file to a filename associated with said original file.

12. (New) The system of Claim 1, wherein said storage means has a directory structure, said component document being stored in said storage means under a directory associated with said compound document.

13. (New) The system of Claim 12, further comprising:

duplicate storage means for storing said duplicate file, said duplicate storage means having a directory structure identical to the directory structure of said storage means storing said original file.

14. (New) The system of Claim 12, wherein said compound document includes an additional component document, said processing means further for extracting said additional component document from said compound document and storing said additional component document in an additional original file in said storage means under said directory associated with said compound document in a hierarchical format designed to preserve the hierarchical relationship between said component document, said additional component document and said compound document.

15. (New) The system of Claim 14, wherein said component document and said additional component document are stored in a sub-directory of said directory associated with said compound document.

16. (New) The system of Claim 1, wherein said canonical format is the Portable Document Format (PDF), and further comprising:

searching means for enabling full-text searching of said duplicate documents.

17. (New) The system of Claim 1, wherein said compound document is an electronic mail folder, an electronic mail message having one or more attachments thereto, an electronic mail message having one or more additional electronic mail messages embedded therein, an execution file or a zip file.

18. (New) The system of Claim 1, further comprising:

appending means for appending a filename to said original file; and

renaming means for renaming said duplicate file in a sequenced format based on said filename of said original file.

19. (New) The system of Claim 1, further comprising:

selection means for enabling selection of said component document from said compound document for storage in said storage means.

20. (New) The system of Claim 2, further comprising:

receiving means for receiving said original document.

21. (New) The system of Claim 2, further comprising:

notarizing means for determining said notary data associated with the notarization of said original file.

22. (New) The system of Claim 2, further comprising:

additional storage means for storing said notary data as a separate notary file.

23. (New) The system of Claim 2, wherein said conversion means is further for embedding said original file in a blank file having said canonical format upon a determination that said original file cannot be converted into said duplicate file.

24. (New) The system of Claim 10, wherein said embedding means for embedding said notary data associated with said duplicate file into said duplicate file further comprises:

creation means for creating a hole in said duplicate file;

original notarization means for determining said notary data associated with said duplicate file by computing a hash value over the contents of said duplicate file excluding said hole; and

storage means for storing said notary data associated with duplicate file within

said hole.

25. (New) The system of Claim 24, further comprising:

validation means for authenticating said duplicate file using at least said notary data associated with said duplicate file.

26. (New) The system of Claim 25, wherein said validation means further comprises:

extraction means for extracting said notary data associated with said duplicate file from said hole;

validating notarization means for determining new notary data associated with said duplicate file by computing an additional hash value over the contents of said duplicate file excluding said hole; and

comparison means for enabling comparison of said extracted notary data with said new notary data to authenticate said duplicate file.

27. (New) The system of Claim 10, wherein said duplicate file is included in a list of duplicate files, each of said duplicate files in said list of duplicate files being cross-referenced to respective original files included in a list of original files, and further comprising:

culling means for enabling culling of files from said list of duplicate files to produce a culled list of duplicate files;

determining means for determining said original files associated with said duplicate files included in said culled list of duplicate files to produce a culled list of original files;

extracting means for extracting said notary data associated with said original file and said notary data associated with said duplicate file from each of said duplicate files in said culled list of duplicate files;

second conversion means for converting each of said original files in said culled list of original files to a canonical format to produce respective new duplicate files;

second embedding means for embedding said extracted notary data associated with said original file and said extracted notary data associated with said duplicate file into said respective new duplicate files to produce a final set of duplicate files;

notarization means for determining new notary data associated with said new duplicate files and embedding said new notary data within said respective new duplicate files; and

second indexing means for inserting a respective sequence number including part of said new notary data into each of said new duplicate files to sequentially number said new duplicate files.

28. (New) The system of Claim 2, further comprising:

validation means for authenticating said original file from said duplicate file.

29. (New) The system of Claim 28, wherein said validation means further comprises:

determining means for determining said original file from said duplicate file;

extraction means for extracting said notary data associated with said original file from said duplicate file;

notarization means for determining new notary data associated with said original file; and

comparison means for comparing said new notary data with said extracted notary data to authenticate said original file.

30. (New) A computer system for securely duplicating digital documents of disparate types to provide a cryptographically secure link between duplicate ones of the digital documents and their respective original ones of the digital documents, said computer system comprising:

a database for storing said original documents in original files, each of said original files containing no more than one of said original documents, each of said original files having a respective original format, said database further for storing said duplicate documents in duplicate files, each of said duplicate files containing one of said duplicate documents, each of said duplicate files having a canonical format; and

a processor for executing software routines configured to convert said respective original format of each of said original files to said canonical format associated with said respective duplicate files, embed respective original notary data associated with said original files into said duplicate files and insert a respective unique sequence number into each of said duplicate files to sequentially number said duplicate files, each said unique sequence number including at least a portion of said original notary data associated with said respective duplicate file.

31. (New) The computer system of Claim 30, wherein at least one of said original documents is a component document of a compound document, said software routines being further configured to extract said component document from said compound document and store said component document in one of said original files.

32. (New) The computer system of Claim 31, wherein said original files are stored in an originals repository of said database and said duplicate files are stored in a duplicates repository of said database, said originals repository and said duplicates repository having identical directory structures, said component document being stored under a directory associated with said compound document in said originals repository and said duplicates repository.

33. (New) The computer system of Claim 32, wherein said duplicates repository has multiple storage bins for storing said duplicate files.

34. (New) The computer system of Claim 30, further comprising:

an input device connected to provide said original documents to said computer system.

35. (New) The computer system of Claim 30, wherein said canonical format is the Portable Document Format (PDF).

36. (New) The computer system of Claim 35, wherein each of said duplicate documents has a Root Dictionary field therein, said software routines being further configured to create a new Dictionary associated with said computer system, store said new Dictionary in said Root Dictionary field of each of said duplicate documents and insert said original notary data for each of said duplicate documents into said respective new Dictionary.

37. (New) The computer system of Claim 30, wherein said original notary data for a select one of said original files includes at least a digital fingerprint associated with said select original file, a timestamp indicating the time said digital fingerprint was obtained and an identifier, said sequence number for said select original file including said identifier.

38. (New) The computer system of Claim 30, wherein said software routines are further configured to insert said respective unique sequence number as a footer on the bottom of each page of said duplicate documents.

39. (New) The computer system of Claim 30, wherein said software routines are further configured to embed respective duplicate notary data associated with each of said duplicate files into said canonical format of each of said duplicate files.

40. (New) The computer system of Claim 39, wherein said software routines are further configured to create a hole in each of said duplicate files, determine said duplicate notary data associated with each of said duplicate files by computing hash values over the contents of each of said duplicate files excluding said hole and store said duplicate notary data for each of said duplicate files within said respective hole.

41. (New) The computer system of Claim 40, wherein said software routines are further configured to extract said duplicate notary data for a select one of said duplicate files from said respective hole, determine new notary data associated with said select duplicate file by computing an additional hash value over the contents of said duplicate file excluding said hole and comparing said extracted notary data with said respective new notary data to authenticate said select duplicate file.

42. (New) The computer system of Claim 30, wherein said database further stores a log file containing an original filename for each of said original files and a sequenced filename for each of said duplicate files, each of said original filenames being cross-referenced to said respective sequenced filename.

43. (New) The computer system of Claim 30, wherein said software routines are further configured to determine a select one of said original files from said respective duplicate file, extract said original notary data from said duplicate file associated with said select original file, determine new notary data associated with said select original file and compare said new notary data with said extracted notary data to authenticate said select original file.

44. (New) The computer system of Claim 30, further comprising:

an output device connected to receive data related to said software routines and output said data to a user;

a user interface connected to provide instructions for executing said software routines to said processor; and

an application program interface of said software routines configured to solicit said instructions and provide said data to said output device.

45. (New) The computer system of Claim 44, wherein said application program interface is further configured to present one or more views to the user via said output device, each of said views containing one or more options for the user, said instructions provided by said user interface device including one or more selected ones of said options.

46. (New) The computer system of Claim 45, wherein said options include one or more of converting said original files to said duplicate files, validating one or more of said original files, validating one or more of said duplicate files, culling said duplicate files to produce a final duplicates repository, assigning exhibit numbers to said duplicate files, producing the final duplicates repository for delivery, producing reports related to one or more of said original files and said duplicate files, listing the mapping between said original files and said duplicate files, displaying one or more of said original files and said duplicate files and listing said sequence numbers.

47. (New) A duplicate file having a canonical format, comprising:

a duplicate digital document of an original digital document in an original file having an original format;

embedded original notary data associated with said original file;

embedded duplicate notary data associated with said duplicate file; and

a unique sequence number including at least a portion of said original notary data to provide a cryptographically secure link between said duplicate file and said original file.

48. (New) The duplicate file of Claim 47, further comprising:

a Root Dictionary field within said duplicate document having a new Dictionary therein, said original notary data being included within said new Dictionary.

49. (New) The duplicate file of Claim 47, further comprising:

a hole within said duplicate document for storing said duplicate notary data, said duplicate notary data being determined from a hash value computed over the contents of said duplicate file excluding said hole.

50. (New) A system for validating the authenticity of digital documents of disparate types, comprising:

storage means for storing a duplicate file containing a duplicate document of an original document in an original file having an original format, said duplicate file having a canonical format;

embedding means for embedding notary data associated with said duplicate file within said duplicate file; and

validation means for authenticating said duplicate file using at least said notary data associated with said duplicate file.

51. (New) The system of Claim 50, wherein said embedding means for embedding said notary data associated with said duplicate file into said duplicate file further comprises:

creation means for creating a hole in said duplicate file;

original notarization means for determining said notary data associated with said duplicate file by computing a hash value over the contents of said duplicate file excluding said hole; and

storage means for storing said notary data associated with duplicate file within said hole.

52. (New) The system of Claim 51, wherein said validation means further comprises:

extraction means for extracting said notary data associated with said duplicate file from said hole;

validating notarization means for determining new notary data associated with said duplicate file by computing an additional hash value over the contents of said duplicate file excluding said hole; and

comparison means for enabling comparison of said extracted notary data with said new notary data to authenticate said duplicate file.

53. (New) A system for validating the authenticity of an original document from a duplicate document of said original document, comprising:

storage means for storing an original file containing said original document and a duplicate file containing said duplicate document, said original file having an original format, said duplicate file having a canonical format;

embedding means for embedding notary data associated with said original file within said duplicate file; and

validation means for authenticating said original file using at least said notary data associated with said original file.

54. (New) The system of Claim 53, wherein said validation means further comprises:

determining means for determining said original file from said duplicate file;

extraction means for extracting said notary data associated with said original file from said duplicate file;

notarization means for determining new notary data associated with said original file; and

comparison means for comparing said new notary data with said extracted notary data to authenticate said original file.

55. (New) A method for duplicating digital documents of disparate types for facilitating searching of such documents, comprising the steps of:

determining whether an original document is a component document of a compound document;

if said original document is a component document, extracting said original document from said compound document;

storing said original document in an original file within a computer system, said original file being in an original format; and

converting said original file from said original format to a canonical format, thereby generating a duplicate file containing a duplicate document of said original document, whereby the searching of such documents is facilitated.

56. (New) The method of Claim 55, wherein said step of storing further comprises the step of:

storing said original file and said duplicate file in identical directory structures.

57. (New) The method of Claim 56, wherein said compound document includes an additional component document, and further comprising the steps of:

extracting said additional component document from said compound document; and

storing said additional component document in an additional original file under a directory associated with said compound document in a hierarchical format designed to preserve the hierarchical relationship between said component document, said additional component document and said compound document.

58. (New) The method of Claim 57, wherein said step of storing said additional component document further comprises the step of:

storing said component document and said additional component document in a sub-directory of said directory associated with said compound document.

59. (New) The method of Claim 55, wherein said canonical format is the Portable Document Format (PDF), and further comprising the step of:

enabling full-text searching of said duplicate documents.

60. (New) The method of Claim 55, further comprising the steps of:

appending a filename to said original file; and

renaming said duplicate file in a sequenced format based on said filename of said original file.

61. (New) The method of Claim 55, further comprising the step of:

enabling selection of said component document from said compound document for file conversion and storage.

62. (New) A method for securely duplicating digital documents of disparate types, said method comprising the steps of:

storing at least one original file, each containing no more than one original document, within a computer system, said original file being in an original format;

converting said original file from said original format to a canonical format thereby generating a duplicate file containing a duplicate document of said original document;

embedding original notary data associated with said original file into said duplicate file, said original notary data being capable of authenticating said original file; and

inserting a unique sequence number including at least a portion of said original notary data into said duplicate file to provide a cryptographically secure link between said duplicate document and said original document.

63. (New) The method of Claim 62, wherein said original document is a component document of a compound document, and further comprising the steps of:

extracting said component document from said compound document; and

storing said component document in said original file under a directory associated with said compound document.

64. (New) The method of Claim 62, further comprising the step of:

storing said duplicate file in said computer system in a directory format identical to a directory format that said original file is stored in.

65. (New) The method of Claim 62, wherein said canonical format is the Portable Document Format (PDF).

66. (New) The method of Claim 65, wherein said duplicate document has a Root Dictionary field therein, and further comprising the steps of:

creating a new Dictionary associated with said computer system;

storing said new Dictionary in said Root Dictionary field; and

inserting said original notary data into said new Dictionary.

67. (New) The method of Claim 62, wherein said original notary data includes at least a digital fingerprint associated with said original file, a timestamp indicating the time said digital fingerprint was obtained and an identifier, said sequence number including said identifier.

68. (New) The method of Claim 62, wherein said step of inserting further comprises the step of:

inserting said unique sequence number as a footer on the bottom of each page of said duplicate document.

69. (New) The method of Claim 62, further comprising the step of:

embedding duplicate notary data associated with said duplicate file into said canonical format of said duplicate file, said duplicate notary data being capable of authenticating said duplicate file.

70. (New) The method of Claim 69, wherein said step of embedding said duplicate notary data further comprises the steps of:

creating a hole in said duplicate file;

determining said duplicate notary data associated with said duplicate file by computing a hash value over the contents of said duplicate file excluding said hole; and

storing said duplicate notary data associated with duplicate file within said hole.

71. (New) The method of Claim 70, further comprising the step of:

authenticating said duplicate file using at least said duplicate notary data associated with said duplicate file.

72. (New) The method of Claim 71, wherein said step of authenticating further comprises the steps of:

extracting said notary data associated with said duplicate file from said hole;

determining new notary data associated with said duplicate file by computing an additional hash value over the contents of said duplicate file excluding said hole; and

enabling comparison of said extracted notary data with said new notary data to authenticate said duplicate file.

73. (New) The method of Claim 69, wherein said duplicate file is included in a list of duplicate files, each of said duplicate files in said list of duplicate files being cross-referenced to respective original files included in a list of original files, and further comprising the steps of:

enabling culling of files from said list of duplicate files to produce a culled list of duplicate files;

determining said original files associated with said duplicate files included in said culled list of duplicate files to produce a culled list of original files;

extracting said original notary data associated with said original file and said duplicate notary data associated with said duplicate file from each of said duplicate files in said culled list of duplicate files;

converting each of said original files in said culled list of original files to a canonical format to produce respective new duplicate files;

embedding said extracted notary data associated with said original file and said extracted notary data associated with said duplicate file into said respective new duplicate files to produce a final set of duplicate files;

determining new notary data associated with said new duplicate files and

embedding said new notary data within said respective new duplicate files; and

inserting a respective sequence number including part of said new notary data into each of said new duplicate files to sequentially number said new duplicate files.

74. (New) The method of Claim 62, further comprising the step of:

mapping a sequenced filename associated with said duplicate file to a filename associated with said original file.

75. (New) The method of Claim 62, wherein said step of converting further comprises the step of:

embedding said original file in a blank file having said canonical format upon a determination that said original file cannot be converted into said duplicate file.

76. (New) The method of Claim 62, further comprising the step of:

authenticating said original file from said duplicate file.

77. (New) The method of Claim 76, wherein said step of validating further comprises the steps of:

determining said original file from said duplicate file;

extracting said original notary data associated with said original file from said duplicate file;

determining new notary data associated with said original file; and

comparing said new notary data with said extracted original notary data to authenticate said original file.

78. (New) A method for validating the authenticity of digital documents of disparate types, comprising the steps of:

retrieving a duplicate file containing a duplicate document of an original document in an original file having an original format, said duplicate file having a canonical format, said duplicate file further having notary data associated with said duplicate file embedded within said duplicate file; and

authenticating said duplicate file using at least said notary data associated with said duplicate file.

79. (New) The method of Claim 78, wherein said notary data is embedded into a hole within said duplicate file, said notary data being determined by computing a hash value over the contents of said duplicate file excluding said hole.

80. (New) The method of Claim 79, wherein said step of authenticating further comprises the steps of:

extracting said notary data associated with said duplicate file from said hole;

determining new notary data associated with said duplicate file by computing an additional hash value over the contents of said duplicate file excluding said hole; and

enabling comparison of said extracted notary data with said new notary data to authenticate said duplicate file.

81. (New) A method for validating the authenticity of an original document from a duplicate document of said original document, said method comprising the steps of:

retrieving a duplicate file containing a duplicate document of an original document in an original file having an original format, said duplicate file having a canonical format, said duplicate file further having notary data associated with said original file embedded within said duplicate file; and

authenticating said original file using at least said notary data associated with said original file.

82. (New) The method of Claim 81, wherein said step of authenticating further comprises the steps of:

determining said original file from said duplicate file;

extracting said notary data associated with said original file from said duplicate file;

determining new notary data associated with said original file; and

comparing said new notary data with said extracted notary data to authenticate said original file.

83. (New) A duplicate document of an original document, comprising:

at least one page;

a footer at the bottom of each said at least one page; and

a unique sequence number inserted in said footer, said unique sequence number including at least a portion of notary data associated with the original document to provide a cryptographically secure link between the duplicate document and the original document.